

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

Title: Military Deception in Counterinsurgency Operations

by

Christine A. Mau, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: LtCol David Kirkendall

Maxwell Air Force Base, Alabama

December 2009

Report Documentation Page			<i>Form Approved OMB No. 0704-0188</i>	
<p>Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p>				
1. REPORT DATE 01 DEC 2009	2. REPORT TYPE	3. DATES COVERED 00-00-2009 to 00-00-2009		
4. TITLE AND SUBTITLE Military Deception in Counterinsurgency Operations		5a. CONTRACT NUMBER		
		5b. GRANT NUMBER		
		5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S)		5d. PROJECT NUMBER		
		5e. TASK NUMBER		
		5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Air Force Institute of Technology, 2950 Hobson Way, WPAFB, OH, 45433-7765		8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)		
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited				
13. SUPPLEMENTARY NOTES				
14. ABSTRACT MILDEC can bring about distinct advantages to a military force and can be just as valuable in COIN as it is in conventional operations. This paper will provide a brief background on COIN operations and military deception and present ways to effectively combine the two.				
15. SUBJECT TERMS				
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 12
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified	19a. NAME OF RESPONSIBLE PERSON	

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Introduction

The current wars in Iraq and Afghanistan have reemphasized the reality that an overwhelming combined arms force cannot win a counterinsurgency (COIN). The International Security Assistance Force (ISAF) Commander's guidance recognizes this truth admitting that the US military's instinctive conventional approach is self-defeating.¹ The US military was slow to adapt to COIN warfare in Iraq and Afghanistan and only this year did the US Government and Joint Chiefs of Staff issue guidance regarding such operations. However, the US Government, joint, and service publications do not adequately address the use of military deception (MILDEC) in COIN operations. MILDEC can bring about distinct advantages to a military force and can be just as valuable in COIN as it is in conventional operations. This paper will provide a brief background on COIN operations and military deception and present ways to effectively combine the two.

Counterinsurgency

COIN operations require a major shift in the mindset of the US military. Since inception, the US military has primarily trained and equipped for conventional warfare. Galula describes the major difference as "the primary challenge of conventional warfare is massing firepower at the appropriate place and time to destroy the enemy, the key to success in counterinsurgency is massing intelligence derived from the local population to identify the enemy."² As stated in the ISAF Commander's COIN Guidance, "We will not win simply by killing insurgents."³ To better understand it, the following paragraphs will define and discuss theories and principles of COIN.

To begin with, COIN is essentially the opposing force of an insurgency. An insurgency is an indigenous threat that uses "subversion and violence to seize, nullify, or challenge political control of a region."⁴ The insurgent's aim is to influence and control the population by

weakening government control and legitimacy. Joint Publication (JP) 3-24 defines COIN as “Comprehensive civilian and military efforts taken to defeat an insurgency and to address any core grievances.”⁵ To win a COIN, the government must secure and control the local population.⁶ This requires reform to ensure a legitimate, accountable government meets the population’s economic needs, and provides security and social services for the people.

JP 3-24 lists 13 principles of COIN that provide focus on how to conduct COIN successfully. The principles and a brief description are listed below.

- Counterinsurgents Must Understand the Operating Environment
 - Political, military, economic, social, information, and cultural aspects
- Legitimacy Is the Main Objective
 - Foster development of effective governance by a legitimate government
- Unity of Effort is Essential
 - Among Department of Defense, Department of State and Host Nation (HN)
- Political factors are Primary
 - Political objectives must guide the military’s approach
- Intelligence Drives Operations
 - Effective COIN is shaped by timely, specific, and reliable intelligence
- Insurgents Must be Isolated from Their Cause and Support
 - It’s more effective to separate an insurgency from the population than to kill or capture insurgents
- Security Under the Rule of Law is Essential
 - Replace military operations with law enforcement quickly and establish a legal system in line with local culture and practices
- Counterinsurgents Should Prepare for a Long-Term Commitment
 - Insurgencies are protracted by nature, often lasting for years or decades
- Manage Information and Expectations
 - Use Information Operations inform the population and set realistic expectations which will build support for and limit discontent with the COIN
- Use the Appropriate Level of Force
 - Use precise and tailored forces to carefully target insurgents and avoid collateral damage as much as possible
- Learn and Adapt
 - Insurgents are agile; every unit needs to be able to make observations, draw and apply lessons, and assess results
- Empower the Lowest Levels
 - Use a centralized vision and decentralized execution with clear and concise rules of engagement
- Support the Host Nation
 - Assist the HN government but ultimately, it has to win on its own

The most important theory in COIN operations is that the population and its allegiance is the center of gravity. The insurgents become a secondary objective.⁷ Therefore, the COIN force must earn the trust and support of the people to isolate the insurgents. This is done by word and deed but, according to Galula, the strategically decisive factor in COIN is the control of information.⁸ Another important concept is that insurgencies often lack a centralized, hierarchical command structure and are typically organized as complex, flat networks enabled by communications technology.⁹ Capturing or killing one insurgent is not likely to have any effect other than to create several more. Still, COIN forces must understand the dynamics of the insurgency to assess its strengths and weaknesses.¹⁰ These dynamics include leadership, objectives, ideology, organizational and operational approaches, external and internal support, and phasing and timing.¹¹

Ultimately, insurgents have an asymmetric advantage over counterinsurgents resulting “from the very nature of the war, from the disproportion of strength between the opponents at the outset, and from the difference in essence between their assets and their liabilities.”¹² They do not have to fight fair, nor do they have to deliver on their promises to the people. COIN forces “should always be looking for potential fracture lines where the coincidence of interests between the ideological leadership and a particular part of the insurgent network is weakest.”¹³ Other aspects of an insurgency that can be both a strength and a vulnerability which a COIN should try to exploit are “secrecy, recruitment and message, base of operations, external support, finances, internal divisions, maintaining momentum, defectors and informants, attrition of human resources and leadership.”¹⁴

Military Deception

Deception in warfare is as old as armed conflict itself. The great military theorist Sun Tzu

said, “All warfare is based on deception.”¹⁵ However, for the US, MILDEC has been undervalued as a tool for friendly forces in doctrinal manuals and during training exercises, where it is often viewed as an ancillary activity.” As Air Force LtCol Edwards states in his Naval War College paper, “Except for the WWII years, the US has not been a great practitioner of deception arts and sciences.”¹⁶ This perhaps is due to the incorrect perception that deception is unethical or is something that only weaker forces must resort to. However, this undervalued capability can bring about distinct advantages during all phases of various military operations. The following paragraphs will provide a definition for, and discuss the key theories and principles of MILDEC.

JP 3-13.4 defines MILDEC as “those actions executed to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.”¹⁷ To put it succinctly, “hide the real and show the fake.” The critical factor is to influence the deception target, causing him or her to behave in a desired way. MILDEC is applicable to all levels of war but delivers the greatest advantage to friendly forces at the operational and strategic levels. As MILDEC focuses on the information system of a deception target to influence his or her thinking and achieve a desired behavior, it is a subset of Information Operations (IO). Thus, it is fundamentally tied to Operational Security (OPSEC), Psychological Operations (PSYOP), Electronic Warfare (EW), and Computer Network Operations (CNO). These disciplines enable and augment successful MILDEC operations.

Because effective MILDEC may require extensive planning and preparation, it should be incorporated into the early phases of an operation.¹⁸ To be effective, MILDEC planners “must think like the enemy and not project his/her own assumptions and values onto the enemy.”¹⁹

MILDEC planning is an art that requires extensive current intelligence, and a cultural and psychological understanding of the deception target. It also requires operational knowledge of the friendly capabilities at the planner's disposal. JP 3-13.4 list some functions of potential MILDEC efforts. They include:

- Causing ambiguity, confusion, or misunderstanding in adversary perceptions of friendly critical information, which may include: unit identities, locations, movements, dispositions, weaknesses, capabilities, strengths, supply status, and intentions.
- Causing the adversary to misallocate personnel, fiscal, and material resources in ways that are advantageous to the friendly force.
- Causing the adversary to reveal strengths, dispositions, and future intentions.
- Conditioning the adversary to particular patterns of friendly behavior to induce adversary perceptions that can be exploited by the joint force.
- Causing the adversary to waste combat power with inappropriate or delayed actions.

In order to achieve the above functions, the Joint Force Commander (JFC) and MILDEC planner should consider the six MILDEC principles. These principles provide guidance for planning and execution of MILDEC operations.

- 1) **Focus** – the deception must target the adversary decision maker capable of taking the desired action(s)
- 2) **Objective** – the deception must cause an adversary to take (or not to take) specific actions, not just to believe certain things
- 3) **Centralized planning and control** – MILDEC operations should be centrally planned and directed in order to achieve unity of effort
- 4) **Security** – friendly forces must deny knowledge of a force's intent to deceive and the execution of that intent to adversaries
- 5) **Timeliness** – a deception operation requires careful timing
- 6) **Integration** – fully integrate each military deception with the operation that it is supporting

These principles enable successful planning and execution of MILDEC operations to achieve MILDEC functions. Another concept that is important to understanding MILDEC is that all MILDEC operations apply four basic deception techniques. These techniques are feints, demonstrations, ruses, and displays.²⁰ A feint is “an offensive action involving contact with the adversary conducted for the purpose of deceiving the adversary as to the location and/or time of

the actual main offensive action.”²¹ A demonstration is a show of force for deception purposes, similar to a feint but no contact with the enemy is intended. A ruse is a trick of war that involves the deliberate exposure of false or confusing information to the adversary’s intelligence collection system so that he may misinterpret it. Finally, a display is a static portrayal of an activity, force, or equipment intended to deceive the adversary’s visual observation. All MILDEC operations employ one of these techniques in some form or fashion.

However, regardless of the MILDEC technique employed, military forces should obey the Laws of Armed Conflict (LOAC) and laws of warfare set out in the Hague and Geneva Conventions. Generally, speaking, the US military recognizes the latter two laws regardless of whether the US ratified them.²² JP 3-13.4 specifically addresses the unlawful and prohibited deception of perfidy.²³ It lists acts of perfidy as feigning surrender in order to lure the enemy into a trap; misusing protected signs and symbols to injure, kill or capture the enemy; and using false, deceptive, or neutral flags, insignia or uniforms in actual combat.

Using MILDEC in COIN

Given the previous descriptions of COIN and MILDEC, it seems intuitive that combining the two would be advantageous. Many of the key principles such as the need for accurate and timely intelligence, long-term commitment to operations, cultural awareness, and a requirement to manage information apply to both. However, the MILDEC principle of centralized planning and control contradicts the COIN principle of empowering the lowest levels with decentralized execution. Also, the MILDEC principle of timeliness which requires careful timing for an operation will be difficult to achieve in a dynamic COIN environment. Yet, conceptually, a COIN force wants to exploit every advantage possible. For example, since MILDEC enables surprise, which is advantageous to military operations, employing MILDEC to achieve such

during COIN operations would theoretically be a good thing.

However, this requires some serious consideration as the primary objective of a COIN is to win the trust and support of the people while capturing and killing insurgents is the secondary objective. Also, MILDEC doctrinally targets adversary decision makers who may be indistinguishable from the local population and perhaps not matter much to the insurgency given its complex, flat network. This creates a difficult situation because while the JFC must “avoid misleading the new media in a manner that would influence US leadership or the American public, it has become acceptable practice to allow the news media to come to false conclusions about operational plans and intentions that deceive the enemy leadership.”²⁴ Counterinsurgents must also avoid the *perception* of trying to mislead the population or media. As JP 3-24 points out, “Even the slightest appearance of impropriety can undermine the credibility of the COIN force and HN legitimacy.”²⁵ An overall concern is that “deception tactics that have a good chance of success during major combat are often legally and ethically clouded by political and human issues during COIN.”²⁶

In his monograph for the School of Advanced Military Studies, MAJ Thibodeaux states, “MILDEC during COIN should target the insurgency, not the insurgent.”²⁷ His analysis of historical examples proves that MILDEC has been successful at the tactical level inside a COIN environment.²⁸ This success was with using OPSEC vulnerabilities in a ruse to ambush insurgent forces, as well as primarily using pseudo operations. Pseudo operations are those “in which government forces and guerrilla defectors portray themselves as insurgent units.”²⁹ They have proven to be very valuable in collecting intelligence and capturing or killing key individuals to COIN efforts of other countries. But they can cause mistrust in the civilian population and destabilize an area.³⁰ While pseudo operations may be an effective tactic, it is considered by

some to be perfidy and is therefore legally hazardous. The use of double agents in MILDEC is also addressed in many sources from Sun Tzu to recent military papers on MILDEC. This is still a risky, but viable option to collect critical intelligence and perform offensive action against insurgents. A detailed analysis of legal considerations regarding the use of MILDEC in COIN operations is beyond the scope of this paper.

Marine LtCol Cunningham suggests a different approach to MILDEC in COIN that takes advantages of insurgent vulnerabilities in a CNO realm. In his research paper for Air War College, he lists the following additional techniques of MILDEC: exploiting Web Blogs to destroy bloggers credibility, manipulating the insurgent's internet operations to hamper recruiting and fund raising, replicating the programming style of adversary computer programmers, and using honeypots to try to fool cyberattackers and collect data about attack methods thereby enabling better defense against attackers.³¹

Conclusion

As stated in the introduction, the US government, joint and service publications do not adequately address the use of MILDEC in COIN operations. The only significant statement is from JP 3-24 which states, "... deception is difficult in COIN due to the need for transparency with the population."³² Regardless of how it's employed as a weapon, the military must regularly exercise MILDEC to remain proficient.³³ Given the historical ad hoc and underutilized nature of MILDEC in the US military, employing it in the current COIN operations in Iraq and Afghanistan may be even more complicated. However, the use of MILDEC in COIN to achieve operational or tactical advantages has utility, especially in the CNO realm of operations. A thorough risk-benefit analysis will help determine whether MILDEC is more likely to help or hurt COIN operations. Overall, this paper provided a brief background on COIN operations and military deception and presented ways to effectively combine the two.

¹ International Security Assistance Force. ISAF Commander's Counterinsurgency Guidance, 2.

² Galula, David. *Counterinsurgency Warfare: Theory and Practice*, vii.

³ International Security Assistance Force. ISAF Commander's Counterinsurgency Guidance, 1.

⁴ United States Government Interagency Counterinsurgency Initiative. *US Government Counterinsurgency Guide*, 6.

⁵ Joint Publication (JP) 3-24. *Counterinsurgency Operations*, I-2.

⁶ Galula, David. *Counterinsurgency Warfare: Theory and Practice*, viii.

⁷ Gray, Colin S. *Irregular Enemies and the Essence of Strategy: Can The American Way of War Adapt?* 42.

⁸ Galula, David. *Counterinsurgency Warfare: Theory and Practice*, ix.

⁹ Joint Publication (JP) 3-24. *Counterinsurgency Operations*, II-19.

¹⁰ Ibid, xii.

¹¹ Ibid.

¹² Galula, David. *Counterinsurgency Warfare: Theory and Practice*, 3.

¹³ United States Government Interagency Counterinsurgency Initiative. *US Govt COIN Guide*, 15.

¹⁴ Joint Publication (JP) 3-24. *Counterinsurgency Operations*, xiii.

¹⁵ Sun Tzu. *The Art of War*, 66.

¹⁶ Edwards, LtCol Rem B. "Allies in the Shadows: Why We Need Operational Deception," 2.

¹⁷ Joint Publication (JP) 3-13.4. *Military Deception*, I-1.

¹⁸ Ibid.

¹⁹ Martin, Charmaine L. "Military Deception Reconsidered," 10.

²⁰ Joint Publication (JP) 3-13.4. *Military Deception*, I-7.

²¹ Ibid.

²² Caddell, Joseph W. *Deception 101 – Primer on Deception*, 13.

²³ Joint Publication (JP) 3-13.4. *Military Deception*, I-8.

²⁴ Baker, Jeffrey L. "Achieving Operational Deception in the Age of CNN," i.

²⁵ Joint Publication (JP) 3-24. *Counterinsurgency Operations*, xx.

²⁶ Thibodeaux, MAJ Maxwell S. "The Utility of Military Deception during Counterinsurgency," 2.

²⁷ Ibid, 44.

²⁸ Ibid, 42.

²⁹ Cline, Lawrence E. *Pseudo Operations and Counterinsurgency: Lessons from Other Countries*, v.

³⁰ Thibodeaux, MAJ Maxwell S. "The Utility of Military Deception during Counterinsurgency," 16 & 34.

³¹ Cunningham, William R. "Military Deception Operations in the United States Air Force," 17-19.

³² Joint Publication (JP) 3-24. *Counterinsurgency Operations*, V-2.

³³ Edwards, LtCol Rem B. "Allies in the Shadows: Why We Need Operational Deception,"

Bibliography

Baker, Jeffrey L. "Achieving Operational Deception in the Age of CNN." Newport RI: Naval War College, 2003.

Cline, Lawrence E. *Pseudo Operations and Counterinsurgency: Lessons from Other Countries*. Strategic Studies Institute. June 2005.

Caddell, Joseph W. *Deception 101 – Primer on Deception*. Strategic Studies Institute. December 2004. <http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=589>. (accessed 9 December 2009).

Cunningham, William R. "Military Deception Operations in the United States Air Force." Maxwell AFB, AL: Air War College, Feb 2007.

Edwards, LtCol Rem B. "Allies in the Shadows: Why We Need Operational Deception." Newport RI: Naval War College, 2004.

Galula, David. *Counterinsurgency Warfare: Theory and Practice*. Westport, CT: Praeger Publishers, 2006.

Gerwehr, Scott and Russell W. Glenn. *The Art of Darkness*. Santa Monica, CA: RAND 2000.

Gray, Colin S. *Irregular Enemies and the Essence of Strategy: Can The American Way of War Adapt?* Strategic Studies Institute. March 2006. <http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=650> (accessed 9 December 2009).

Grohe, LCDR Edwin J. "Military Deception: Transparency in the Information Age." Newport RI: Naval War College, 2007.

International Security Assistance Force. ISAF Commander's Counterinsurgency Guidance, August 2009.

Joint Publication (JP) 3-13.4. *Military Deception*, 13 July 2006.

Joint Publication (JP) 3-24. *Counterinsurgency Operations*, 5 October 2009.

Martin, Charmaine L. "Military Deception Reconsidered." Monterey, CA: Naval Postgraduate School, June 2008.

Sun Tzu. *The Art of War*. Translated by Samuel B. Griffith. New York, NY: Oxford University Press, 1963.

Thibodeaux, MAJ Maxwell S. "The Utility of Military Deception during Counterinsurgency." School of Advanced Military Studies. Fort Leavenworth, KS: Command and General Staff College. 2007.

United States Government Interagency Counterinsurgency Initiative. *U.S. Government Counterinsurgency Guide*. Bureau of Political-Military Affairs. January 2009. <http://www.state.gov/documents/organization/119629.pdf> (accessed 9 December 2009)

Webb, Maj Michael D. "Creating a New Reality: Information Age Effects on the Deception Process." Maxwell AFB, AL: School of Advanced Air and Space Studies, June 2006.